



**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

North East

CrimeAlert

Keeping Communities in the North East Safe

September 2023



North East CrimeAlert

Keeping Communities in the North East Safe
September 2023

Welcome to the September edition of North East Crime Alert.

A quarterly bulletin produced by the Police Scotland North East Division Crime Reduction Team aimed at keeping you up to date with what's happening in our community.

In this edition of North East Crime Alert:

Detective Sergeant Scott McKay explains the ground breaking work being carried out by Operation Protector in the North East of Scotland.

We explain how to avoid becoming a victim of Concert Ticket fraud.

As students return to University Rental Fraud is on the increase; learn how to avoid becoming a victim.

We have a victims account of how their business fell foul of scammers.

As well as a regular round-up of crime in the North East.

From the latest frauds and scams, to general security measures, each issue will bring you advice on how to keep your property safe.

Crime across Scotland is increasing and criminals are using ever more sophisticated methods. By working in partnership we can make our communities a safer place to live and work.



Operation Protector

is the North East's pioneering multi-agency approach to reducing drug related harm in our communities.

Agencies are working together across Grampian to minimise the risk to those who are vulnerable in our communities and target those causing harm.



The partnerships are made up of representatives from:

- Police Scotland
- British Transport Police
- Aberdeen City, Aberdeenshire and Moray Local Authorities
- The NHS
- Turning Point Scotland
- Alcohol & Drugs Action
- Arrows (Quarriers).

It's important to highlight that no one chooses to be dependent on drugs. Stigma relating to those who use drugs is ever present in our communities.

This makes it extremely difficult for those who are dependant to seek help as often their self-esteem is rock bottom and being segregated, judged and often publically insulted only adds to their feelings of low self-worth. Addressing the stigma attached to the use of controlled drugs is a key objective for 'Operation Protector.'

The operation brings together key people to undertake a number of tasks which contribute to reducing drug related harm namely Assertive Outreach, Community Outreach, Community Safety and Improvement and Enforcement.

Assertive Outreach is undertaken by joint teams from Police, Social Work, Substance Services and Housing and brings real time support to those most vulnerable in our communities. This includes options like medically assisted treatment, support with mental health, housing or cost of living issues.

Community Outreach Multi-agency hubs in the heart of our communities aim to raise awareness of the wider picture associated with drug dependency and the risks of 'cuckooing' and exploitation. Naloxone (a lifesaving medication), other harm reduction materials and food parcels are also provided to those in need.

Community Safety and Improvement is undertaken between Police and Local Authorities. This often focusses on key perpetrators of drug related harm and seeks to reduce the harm they cause by forcing a change in their behaviour by working with the individual to deter criminality.

Enforcement Activity is undertaken by Police in the form of Drug Search Warrants and pre-planned arrests of those involved in committing serious drug related harm and violence. Uniquely every person interacted with during the enforcement work is offered support from a dedicated enforcement support team comprising police, housing and substance support staff.

Since December 2021 the teams have:

Undertaken 2105 multi-agency visits

Over 2500 interactions with the public

Over 3000 addresses visited by Community Safety Teams

96 Drug Search Warrants executed and large quantities of drugs, money and weapons seized

10 'County Lines' exploited children found and safeguarded from further exploitation

2 persons charged with 'County Lines' Child Trafficking Offences

1 high risk offender issued with an ASBO excluding him from the Aberdeenshire area



OLD YEAR
& GUESTS
2 OCTOBER 2018
NELS, CARNEGIE'S BRAT, ABERDEEN
6 // DOORS 1900

Cold Years

& GUESTS

oasis
ABERDEEN EXHIBITION & DOMESTIC
BRIDGE OF DON, ABERDEEN

THE WHO
QUADROPHENIA
AND MORE

SECC - Hall 4
Wednesday
12-June-2013
6:30 pm
Adult
£70.00

DF CONCERTS presents

RADIOHEAD

Plus Special Guests
HALL A, AECC
Bridge of Don, Aberdeen
Thursday 20th November 1995
£15.00 In Advance
(Subject to booking fee)
Doors Open 6:30 p.m.
Right Of Admission Reserved
No Age Restriction, Separate Bar In Venue

PERFORMING ARTS

Music Hall
Mon 02 Nov Door Time: 7:00pm
Standard - £27.50
DF Concerts Presents

Teenage Fanclub
Plus Special Guests
Doors - 8pm

Ticket fraud don't get caught out

STANDING
ENTER VIA WEST
ENTRANCE

39 ENTERTAINMENT
PAUL WELCHER
PLUS SUPPORT
AECC PRESS & JOURNAL AREA
DOORS 6:30 PM
SUN 5TH DEC 2013

AECC PRESS & JOURNAL AREA

DF Concerts Presents
The Killers Live in concert

WEDNESDAY
21st FEB 07
Doors 6:30 PM

STANDING AREA
ADMIT ONE
#431

BOOK ONLINE



Avoiding Ticket Fraud

A Guide for Concert-Goers

The excitement of attending a live concert can quickly turn into disappointment if you become a victim of ticket fraud. As the popularity of concerts continues to rise so do fraudulent ticket schemes. However, by being vigilant and following a few essential guidelines, you can significantly reduce the risk of falling prey to ticket fraud. This article provides valuable advice on how to avoid ticket fraud and highlights the key factors to consider when purchasing concert tickets.

Purchase from Authorised Sources

To minimise the risk of ticket fraud, always buy tickets from authorised sources. Start by checking the official website of the concert venue or the artist performing. They often partner with reputable ticketing companies, ensuring the authenticity and validity of the tickets. Avoid purchasing tickets from suspicious third-party websites or individuals, as they are more likely to be involved in fraudulent activities.

Verify the Seller's Reputation

If you decide to purchase tickets from a secondary market or individual sellers, research their reputation beforehand. Look for feedback/reviews from other buyers and consider using well-established platforms that offer buyer protection. Reliable platforms often have measures in place to prevent fraudulent activities and will intervene if any issues arise.

Beware of Overly Attractive Deals

While discounted tickets can be tempting, be cautious of deals that seem too good to be true. Fraudsters often lure unsuspecting buyers with significantly lower prices to exploit their trust. Always compare ticket prices across multiple sources to get a better understanding of the market value.

Double-Check Ticket Details

Before making a purchase, carefully review the ticket details to ensure their authenticity. Check for accurate event information, including the date, time, and venue. Pay attention to the seating section or assigned seats, as this can be an indicator of fraudulent tickets. If the seller refuses to provide essential details or seems evasive, it's best to avoid the transaction.

Use Secure Payment Methods

When purchasing tickets online prioritise secure payment methods to safeguard your financial information. Credit cards and reputable online payment platforms offer additional protection against fraudulent transactions. Avoid paying with cash, wire transfers, or unsecured payment methods as they offer little to no recourse in case of fraud.

Be Wary of E-Tickets

While electronic tickets (e-tickets) are convenient, they can also be prone to fraud. When purchasing e-tickets, ensure you receive them through official channels or reputable ticketing platforms. Be cautious of sellers who send scanned or photocopied tickets, as these can be easily duplicated or invalidated. Always verify the authenticity of e-tickets with the ticket issuer or venue directly.

Educate Yourself about Ticketing Policies

Familiarise yourself with the ticketing policies of the event and the ticketing company. Understand the terms and conditions, refund policies, and any restrictions on reselling or transferring tickets. Being aware of these policies will help you identify fraudulent practices, such as non-transferable tickets being sold by unauthorised sellers.

Attending concerts is an exhilarating experience, and by following these guidelines, you can reduce the risk of ticket fraud significantly. Always purchase tickets from authorised sources, verify the seller's reputation, double-check ticket details, use secure payment methods, and educate yourself about ticketing policies. By staying informed and vigilant you can ensure that your concert experiences are memorable for all the right reasons.

Useful Links

www.star.org.uk

Society of ticket agents and retailers

www.ticketmaster.co.uk

Online ticket sales

www.fca.org.uk

Financial Conduct Authority

www.mpsonline.org.uk

Remove your address from mass marketing mailing lists

www.tpsonline.org.uk

Remove your telephone number from mass marketing call lists



The North East Crime Reduction Team once again spent two days at Turriff Show.

The Police Scotland JCB attracted a lot of attention and served to highlight the issues of plant and fuel theft.

Many thanks to Scottish Land and Estates for hosting the team within their gazebo.





Rental Fraud

It's on the increase, stop and consider these tips to avoid fraudsters taking your deposit.

Property rental fraud is on the increase and with the new terms at University about to start demand is sure to be high to secure that new rental home.

Avoiding becoming a victim of fraud is crucial when seeking to rent a domestic property in Scotland. Rental fraud can lead to financial loss, stress and legal complications. To safeguard yourself from these scams follow these precautionary steps:

Work with Reputable Agents and Landlords

Deal only with established letting agents or landlords with a proven track record. Look for registered members of accredited organizations such as the Scottish Association of Landlords (SAL) or the National Approved Letting Scheme (NALS).

Verify Property Ownership

Before committing to a rental agreement, verify the property's ownership through the Land Register of Scotland. This will ensure that the person you're dealing with is the legitimate owner or authorized representative.

Visit the Property in Person

Never agree to rent a property without visiting it in person. Scammers often rely on remote transactions to avoid exposure. Physically inspect the property and its surroundings to ensure its legitimacy.

Don't Pay Upfront Fees

Be cautious if asked to pay substantial upfront fees, especially before viewing the property. A common scam involves requesting money for administrative charges, background checks, or holding deposits before any formal agreements are made.

Request Proper Documentation

Legitimate landlords and agents should provide a formal lease agreement outlining terms and conditions. Read the agreement thoroughly and clarify any doubts before signing. Be wary if pressured to sign without adequate review.

Beware of Unrealistic Offers

If a rental property's price seems too good to be true, it probably is. Scammers often use unrealistically low prices to lure victims into their traps.

Use Secure Payment Methods

When making payments, use secure methods like bank transfers. Avoid cash transactions as they leave no paper trail and are difficult to trace in case of disputes. Never wire transfer money or use cryptocurrency to secure property.

Check for Reviews and References

Look for online reviews of the letting agent or landlord and ask for references from previous tenants. Genuine landlords and agents will be more than willing to provide such information.

Trust Your Instincts

If something feels off or raises suspicions during your interactions, trust your instincts and proceed with caution. It's better to walk away from a potential scam than to risk your finances and personal information.

Avoid Unusual Payment Requests

Be wary of requests to send money through unconventional channels like wire transfers, cryptocurrency, or money transfer services. Legitimate landlords and agents usually accept standard payment methods.

Be Cautious of Remote Transactions

If you're unable to visit the property in person, consider enlisting a trusted friend or family member to verify its legitimacy on your behalf.

Guard Your Personal Information

Scammers often request personal information for background checks or other reasons. Avoid sharing sensitive data like Social Security numbers, passport copies, or financial details until you're certain of the legitimacy of the transaction.

Research the Landlord/Agent: Research the landlord or letting agent online to ensure they have a legitimate online presence. Scammers often use fake names and profiles.

Report Suspicious Activity

If you encounter a potential rental scam report it to the Police. This can help prevent others from falling victim to the same scam.

By following these precautionary measures and staying vigilant, you can significantly reduce the risk of becoming a victim of rental fraud.

Remember that thorough research, common sense and careful scrutiny can go a long way in safeguarding your interests during the whole rental process.

Useful Links

www.scottishlandlords.com	Scottish association of landlords
www.ros.gov.uk	Land register of Scotland
www.fca.org.uk	Financial Conduct Authority
www.royalmail.com	Report nuisance mail



Scam Update #12

Vishing



Vishing is short for voice phishing, where attackers use phone calls to deceive individuals into divulging sensitive information such as passwords, credit card details or personal identification. To safeguard yourself against vishing attacks, it's essential to adopt a proactive and cautious approach.

Caller Verification

Always verify the identity of the caller before sharing any personal or sensitive information. If someone claims to be from a legitimate organisation, end the call and independently find the official contact information for that organisation to confirm the call's legitimacy.

Never Share Sensitive Information

Legitimate institutions will never ask for sensitive information like passwords, Social Security numbers, or credit card details over the phone. If a caller requests such information hang up immediately.

Stay Cautious of Urgent Requests

Attackers often use urgency as a tactic to pressure victims into making hasty decisions. Whether it's a time-sensitive offer, a legal threat, or a pending financial transaction, take a moment to verify the information independently.

Use Two-Factor Authentication (2FA)

Enable 2FA on your accounts whenever possible. This adds an extra layer of security by requiring a second form of verification beyond just your password. Even if an attacker has your password they won't be able to access your account without the second factor.

Caller ID Spoofing Awareness

Attackers can manipulate caller ID information to make it appear as if the call is coming from a legitimate source. Remember that caller ID is not fool-proof and don't solely rely on it to determine a call's authenticity.

Trust Your Instincts

If something feels off about a phone call - whether it's the tone, the information being requested, or the overall context - trust your instincts and end the call.

What can you do?

In a digital landscape where cyber threats continue to evolve, staying vigilant and informed is crucial to protecting yourself from vishing attacks. By combining these strategies with a healthy dose of

scepticism, you can significantly reduce the risk of falling victim to vishing cybercrime and maintain greater control over your personal information.



In our regular series bringing you first hand experiences of victims of crime from across the North East we look at a local business who fell victim to a high value fraud.

A North East oil service company were recently the victim of a purchase fraud costing £30,000. Director 'Andrew' provided details of how it came about.

'Our Sales Team was contacted online by a potential new customer, which is not unusual, we get several new customers every month and around 30% of our business is online. The enquiry was official and very professional, the client was checked and found to be on LinkedIn.

The part number requested was not a company manufactured product and therefore we had to source it online. We contacted a supplier online, they confirmed the parts were in stock, so a purchase order was placed. However as a new customer, the supplier issued a pro-forma invoice and full payment was requested in advance, not unusual, however it later transpired that unfortunately the supplier was in-actual fact fake.

The part was ordered and the customer advised accordingly. They informed us that they would come to our premises to check the items and ensure everything was correct and in order.

7-10 days later and prior to their visit we got another order from the same company but for another part costing £100k. I became very suspicious and started to dig deeper. Further checks on LinkedIn found the profile had been stolen. On investigating the sales procedure I found no actual verbal communication had taken place and when the banking details were checked I found the bank was based in Dubai.

When we went to cancel the order we found the supplier and customer were both fake.

As a company we are often more wary of fraudulent customers than suppliers so this has been a steep learning curve for us all. All the communications and fake documents were extremely professional and showed real attention to detail.'

What has been changed since?

Increased staff training in all matters cyber related.

Review of all online insurance policies

Ensure all customers are phoned and verified in person.

Now have a much stricter policy on all purchases.



**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

What's happening in Aberdeenshire

Portlethen

On 20 July two males wearing dark clothing and balaclavas were disturbed attempting to steal a motorbike from a property on Cairngrassie Drive, Portlethen.

On 25 July a Portlethen resident fell victim to a dating app fraud losing over £27,000. Fraudsters claimed the money was for medical supplies in Ukraine.

On 1 August a Portlethen resident lost £4,200 placing a deposit for a campervan advertised for sale on Facebook Marketplace. The campervan was never delivered.

Kinneff

On 26 July a Giant electric bicycle valued at £2500 was stolen from outside a property in Kinneff.

Aboyne

Between 12 and 16 June two mountain bikes were stolen from a secure bike shed at Aboyne Primary School.

Newmachar

On 21 July 450 litres of diesel was stolen from two vehicles on a building site in Newmachar.

On 18 July a KTM motorbike valued at £4000 was stolen and later recovered from a property at Canmore Gardens, Newmachar.

Maud

On 25 August a resident of Maud fell victim to an Apple Gift Card fraud and lost £400 having received an email appearing to be from a friend.

Strichen

On 10 August a resident of Strichen lost £1400 in an investment fraud having been contacted via Facebook by fraudsters pretending to be a known friend.

Kincardine & Mearns

Two men aged 22 and 24 have been arrested and charged in connection with housebreakings in Blairs, Banchory-Devenick, Findon and Portlethen.

Huntly

On 16 July £1500 of kerosene and diesel were stolen from a rural property on the Ythanwells area.

Stuartfield

On 26 July a resident of Stuartfield lost £900 in a phone scam. Fraudsters pretended to be from BT and persuaded the victim to provide banking details.

Rhynie

On 10 July a resident from Rhynie lost £4850 in a Whatsapp fraud. Fraudsters pretended to be a family member and persuaded the victim to transfer the money at a local bank.



**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

What's happening in Moray

Break-ins - Buckie

Officers in Buckie are appealing for information after emergency flares were set off at Buckie Harbour on Monday 21 August leading to a full search of the area being carried out by emergency services. This follows two youths having broken into a shipyard on Commercial Street around 8.45pm on Sunday 20 August.

Theft of scrap metal - Keith

Around 8pm on Friday 14 July scrap metal was stolen from the Blackhillock substation near Keith by two males in a white Transit style van. About 3pm on Sunday 23 July, near to the Moray West substation site near Keith, two males were disturbed attempting to steal copper wire. A white Ford Transit van drove off towards the A96 losing one of the vans door.

Break-in - Buckie

Police in Buckie are appealing for information following a break-in to a garage on Moray lane, Buckie. The incident took place around 5am on Sunday 2 July.

Break-in – Elgin

Police in Elgin are appealing for information following a Housebreaking with intent to steal at Greenfingers, Garden Nursery, Cooper Park, Elgin. Between 3.45pm on Monday 3 July and 8.30am on Tuesday 4 July the site was entered and a caravan broken into.

Attempted theft of car - Lossiemouth

Police are appealing for information after an attempt was made to steal a car from a garage on Elgin Road, Lossiemouth. The incident took place between 5pm on Thursday 3 August and 11.20 am on Friday 4 August. A window on the car was smashed and attempt made to start the vehicle.

Theft of Fuel – Keith

Police in Keith are appealing for information following the theft of fuel from a farm near Mulben, Keith. Between 11pm on Tuesday 18 July and 5am on Wednesday 19 July 2023, 2000 litres of fuel was taken from the fuel tank located on the farm.



**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

What's happening in Aberdeen

Push Payment Fraud

During May, a 85 year old Aberdeen resident fell victim to an elaborate push payment/safe account fraud, which resulted in him transferring money from numerous accounts into alleged 'safe accounts'. They lost £200,000.

Cryptocurrency Fraud

During May and June a 65 year old man lost his life savings in a crypto currency fraud. Believing his initial investment had increased massively he went on to allow scammers 'remote access' to his computer. He lost £76,000.

Facebook marketplace

Facebook Marketplace continues to be a lucrative area for fraudsters to operate. Many Aberdeen residents have lost out not only by purchasing but also selling on this platform. Look out for sellers offering suspiciously low prices for high priced items, they refuse to meet in person, they try to take the conversation outside of Facebook Messenger, buyers send you prepaid shipping labels, buyers overpay for a product, buyers or sellers ask for your phone number, they don't have a profile photo or want you to pay with a gift card.

Online Employment

In the last few months we have had numerous people lose money to 'online reviewing' jobs. In order to increase income they rely on re-investment. Most victims have went on to lose on average £5000 - £18000.

Fake Evri Fraud

On 27 July an Aberdeen resident received a fake missed delivery message from Evri. It was followed by a fake phonecall stating they had been scammed and to move their money into another 'safe' account. They lost £5000.

Romance Fraud

Over a 6 month period, after meeting a female on a well known 'Dating App,' a 55 year old male was persuaded to invest online through various investment schemes. He went on to lose £38,000.

Kitten Scam

An Aberdeen resident tried to purchase a kitten online from an unregistered company. Having paid an initial fee they went onto to receive numerous bills, but still never received their kitten. They lost £2000.

E-Bike Theft

On 13 August, a Marida electric mountain bike was stolen from Back Wynd, Aberdeen. A poor security lock was easily overcome .

Findon/Marwell Break-ins

Over a 5 day period in August, 6 properties were targeted, sheds, garages and containers were broken into. Power tools, gardening equipment and mountain bikes were stolen.

Drug seizure

On 15 August, a drugs warrant was carried out in the Bridge of Don area of Aberdeen, £330,000 of cannabis was recovered and a 29 year old male was arrested and charged.

Speeding charge

On 30 June, a 40 year old male was caught doing 147mph on the A90 AWPR Aberdeen. He was reported to the Procurator Fiscal.

Ponzi Scheme

A Ponzi Scheme is a scam investment scheme . In July it became apparent an elderly Aberdeen male had been the victim of this crime and had lost over £700,000.

Tool theft

On 27 July, a building works secure cabin in Aberdeen City Centre was broken into and £10,000 of power tools and equipment was stolen.

Keeping Our Communities in the North East Safe

Police Scotland's North East Division covers rural and urban areas in Moray, Aberdeenshire and Aberdeen City. The division has five territorial command areas which have their own dedicated Area Commander, who is responsible for the daily policing function. Each command area is served by a number of community policing teams whose activities are built around the needs of the local community. These teams respond to local calls and look for long term solutions to key issues. They are assisted by the division's Crime Reduction Unit who deliver against

Force and local priorities in a number of areas, including physical and social crime prevention, supporting and enhancing community engagement and creating and sustaining strong and effective partnership working.

Website

www.scotland.police.uk

Twitter

www.twitter.com/NorthEPolice

Facebook

[www.facebook.com/
NorthEastPoliceDivision](http://www.facebook.com/NorthEastPoliceDivision)

North East Division Crime Reduction Team

Moray (Keith)

PC Richard Russell
Richard.russell@scotland.police.uk

Aberdeen City (Nigg)

PC Mark Irvine
Mark.irvine@scotland.police.uk

Aberdeenshire (Stonehaven)

PC Mike Urquhart
Michael.urquhart@scotland.police.uk

Wildlife Crime Officer (Keith)

PC Hannah Corbett
Hannah.corbett@scotland.police.uk



**POLICE
SCOTLAND**
Keeping people safe
POILEAS ALBA